CLAIMS

1. A method of encrypting data which is originally unencrypted, the method comprising:

(a) selecting one or more portions of the unencrypted data to be encrypted;

(b) associating a license with the data portions to be encrypted, the license including license ID data and cryptographic information;

(c) protecting the data portions using cryptographic information of the associated license by

i) directly use the cryptographic information found in the license to encrypt the data portion selected, or

ii) encrypting the data portion selected with a user defined or random encryption key, encrypt this key with the cryptographic information found in the license, and include this encrypted key as a header to the encrypted data; and

(d) replacing each selected originally unencrypted data portion with its corresponding encrypted version of the data portion.

2. The method of claim 1 wherein the data are expressed by a programming language.

3. The method of claim 2 wherein the replaced data portions conform to the syntax of the programming language.

4. The method of claim 3 wherein the replaced data portions are included within a comment field of the programming language.

5. The method of claim 3 further comprising:

(e) including tags in the data to identify the license ID being used in the encryption in step (c), wherein the identifying tags of a license are included within the comment field of the programming language.

6. The method of claim 1 wherein the data are expressed by a syntax-based multimedia data format language.

7. The method of claim 6 wherein the replaced data portions conform to the syntax of the multimedia data format language.

8. The method of claim 7 wherein the replaced data portions are included within a comment field of the multimedia data format language.

9. The method of claim 7 wherein the replaced data portions are included within a header of the multimedia data format language.

10. The method of claim 7 further comprising:

(e) including tags in the data to identify the license ID being used in the encryption in step (c), wherein the identifying tags of a license are included within the comment field of the multimedia data format language.

11. The method of claim 1 wherein the data are expressed by a markup language.

12. The method of claim 11 wherein the replaced data portions are included within a comment field of the markup language.

13. The method of claim 12 further comprising:

(e) including tags in the data to identify the license ID being used in the encryption in step (c), wherein the identifying tags of a license are included within the comment field of the markup language.

14. The method of claim 11 wherein the replaced data portions conform to the syntax of the markup language.

15. The method of claim 1 further comprising:

(e) including tags in the data to identify the license ID being used in the encryption in step (c).

16. The method of claim 15 further comprising:

(f) storing the license data and cryptographic information in a token.

17. The method of claim 16 wherein the protection further includes access control rights, and step (f) further comprises storing the access control rights in the token.

18. The method of claim 16 wherein the license further includes a time constraint.

19. The method of claim 16 wherein the license further includes a number constraint.

20. The method of claim 1 wherein in step (a), at least a portion of the data is not selected for encryption so that after step (c) is completed, the data includes a combination of selected encrypted portions and unselected unencrypted portions.

21. The method of claim 20 further comprising:

(d) creating a rendition of the combination of the encrypted portions and the unencrypted portions.

22. The method of claim 1 wherein the portions of data to be selected in step (a) are manually selected by a user.

23. The method of claim 1 wherein the originally unencrypted data is presented on a user interface display, and the portions of data to be selected in step (a) are selected by highlighting the portions of data on the user interface display.

24. The method of claim 1 wherein the process is repeated with another license, giving a plurality of different encrypted data portions.

25. The method of claim 1 wherein the encrypted data is integrity protected by the use of an encrypted message digest.

26. The method of claim 1 wherein the license is a password-based encryption key.

27. A method for decrypting data that includes one or more portions of encrypted data, the method comprising:

(a) detecting the presence of an encrypted data portion within an original block of data;

(b) accessing license data from a license data memory; and

(c) using the license data obtained from the license data memory to determine if a valid license exists to receive a decrypted version of the encrypted data portion, and if so, then

(i-i) decrypting the encrypted data portion by directly using the cryptographic information of the associated license obtained from the license data memory, or

(i-ii) decrypting the cryptographic key in the header of the encrypted data using cryptographic information of the associated license obtained from the license data memory and decrypt the data portion by using the decrypted cryptographic key; and

(ii) replacing the encrypted data portion with a decrypted version of the data portion.

28. The method of claim 27 wherein step (c) further comprises:

(iii) presenting the decrypted version of the data portions to a display screen.

29. The method of claim 28 wherein the original block of data includes one or more unencrypted portions interspersed within the decrypted portion, and step (c)(iii) further comprises presenting the unencrypted portions and the decrypted portion to the display screen in a single, unified unencrypted manner.

30. The method of claim 29 wherein there are a plurality of different encrypted data portions, each having a unique license, and steps (a)-(c) are repeated for each of the different data portions, and step (c)(iii) further comprises presenting the unencrypted portions and the decrypted portions to the display screen in a single, unified unencrypted manner.

31. The method of claim 29 wherein if the user is determined not to hold a valid license to receive a decrypted version of the encrypted data portion, then step (c)(iii) further comprises presenting only the unencrypted data portions to the display screen in a rendition of the data.

32. The method of claim 27 wherein the data are expressed by a syntax-based multimedia data format language.

33. The method of claim 32 wherein the encrypted data portion conforms to the syntax of the multimedia data format language.

34. The method of claim 33 wherein the encrypted data portion is included within a comment field of the multimedia data format language.

35. The method of claim 32 wherein the encrypted data portion is included within a header of the multimedia data format language.

36. The method of claim 27 wherein the data are expressed by a markup language.

37. The method of claim 36 wherein the encrypted data portion conforms to the syntax of the markup language.

38. The method of claim 37 wherein the encrypted data portion is included within a comment field of the markup language.

39. The method of claim 27 wherein the data are expressed by a programming language.

40. The method of claim 39 wherein the encrypted data portion conforms to the syntax of the programming language.

41. The method of claim 40 wherein the encrypted data portion is included within a comment field of the programming language.

42. The method of claim 27 wherein the license is identified by tags in the data.

43. The method of claim 27 wherein the license data stored in the license data memory and the encrypted data include access control rights, and step (c) further comprises determining if the appropriate access control rights exist to receive a decrypted version of the encrypted data portion.

44. The method of claim 27 wherein the license data stored in the license data memory includes a time constraint, and step (c) further comprises determining if the time constraint is legal within the current time to receive a decrypted version of the encrypted data portion.

45. The method of claim 27 wherein the license data stored in the license data memory includes a number constraint, and step (c) further comprises determining if the number constraint is legal to receive a decrypted version of the encrypted data portion; and if so

(i) decrypt the data portion; and

(ii) decrease the number constraint

46. The method of claim 27 wherein there are a plurality of different encrypted data portions, each having a unique license, and steps (a)-(c) are repeated for each of the

different data portions.

47. The method of claim 25 wherein the data is verified for correct integrity.

48. The method of claim 25 wherein the license data memory resides in a token, and step (b) further comprises accessing the license data and cryptographic information from the token.